



PTO/SB/08B (10-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary) Sheet 2 of 3		Complete if Known	
		Application Number	10/068,295
		Filing Date	February 5, 2002
		First Named Inventor	Mitchell, Oscar
		Group Art Unit	2151
		Examiner Name	
		Attorney Docket Number	501143.000019

RECEIVED

DEC 03 2002

OTHER PRIOR ART - NON PATENT LITERATURE DOCUMENTS			
Examiner Initials ¹	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T ²
lc	C1	MENEZES, A.J., et al "Efficient Implementation" from the Handbook of Applied Cryptography, (Boca Raton, CRS Press, 1997), pp. 591-607.	
lc	C2	DIMITROV, V. and COOKLEV, T., "Two Algorithms for Modular Exponentiation Using Nonstandard Arithmetics" IEICE Trans. Fundamentals, Vol. E78-A, No. 1, January 1995.	
lc	C3	KOC, C.K. and HUNG, C.Y., "Carry-Save Adders for Computing the Product AB Modulo N" Electronics Letters, Vol. 26, No. 13, (June 21, 1990), pp. 899-900	
lc	C4	FREKING, W. L. and PARHI, K.K., "Montgomery Modular Multiplication and Exponentiation in the Residue Number System" Proc. 33rd Asilomar Conf. Signals Systems and Computer, October 1999, pp. 1312-1316.	
lc	C5	TENCA, A.F. and KOC, C.K., "A Scalable Architecture for Montgomery Multiplication" in: KOC, C.K. and PAAR, C., Cryptographic Hardware and Embedded Systems, CHES 99, Lecture Notes in Computer Science, No. 1717, 1998, New York, NY: Springer-Verlag, 1999.	
lc	C6	KOC, C.K. and ACAR, T., "Montgomery Multiplication in GF (2k)" 3rd Annual Workshop on Selected Areas in Cryptography, (August 15-16, 1996), pp. 95-106.	
lc	C7	BAJARD, J.C., et al "An RNS Montgomery Modular Multiplication Algorithm" IEEE Transactions on Computer, Vol. 47, No. 7, (July 1998), pp. 766-776.	
lc	C8	ELDRIDGE, S.E., "A Faster Modular Multiplication Algorithm" International Journal of Computer Math, Vol. 40, (1991), pp. 63-68.	
lc	C9	BOSSALAERS, A., et al "Comparison of Three Modular Reduction Functions" In Douglas R. Stinson, editor, Advances in Cryptology - CRYPTO '93, Vol. 773 of Lecture Notes in Computer Science, (August 22-28, 1993), pp. 166-174.	
lc	C10	MONTGOMERY, P.L., "Modular Multiplication Without Trial Division" Mathematics of Computation, Vol. 44, No. 170 (April 1985), pp. 519-521.	
lc	C11	KOC, C.K., et al "Analyzing and Comparing Montgomery Multiplication Algorithms" IEEE Micro, Vol. 16, Issue 3, (June 1996), pp. 26-33.	

Technology Center 2100

Examiner Signature		Date Considered	12/16/04
--------------------	--	-----------------	----------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.



PTO/SB/08B (10-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO		Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)		Application Number	10/068,295
		Filing Date	February 5, 2002
		First Named Inventor	Mitchell, Oscar
		Group Art Unit	2151
		Examiner Name	
Sheet 3	of 3	Attorney Docket Number	501143.000019

RECEIVED

DEC 03 2002

Technology Center 2100

OTHER PRIOR ART - NON PATENT LITERATURE DOCUMENTS			
Examiner Initials ¹	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T ²
LC	C 12	KORNERUP, P., "High-Radix Modular Multiplication for Cryptosystems" Department of Mathematics and Computer Science, (1993), pp. 277-283.	
LC	C 13	SUNAR, B. and KOC, C.K., "An Efficient Optimal Normal Basis Type II Multiplier" Brief Contributions, IEEE Transactions on Computers, Vol. 50, No. 1, (January 2001), pp. 83-87.	
LC	C 14	KOC, C.K., "Comments on 'Residue Arithmetic VLSI Array Architecture for Manipulator Pseudo-Inverse Jacobian Computation'" Communications, IEEE Transactions on Robotics and Automation, Vol. 7, No. 5, (October 1991), pp. 715-716.	
LC	C 15	SAVAS, E. and KOC, C.K., "The Montgomery Modular Inverse-Revisited" IEEE Transactions on Computers, Vol. 49, No. 7, (July 2000), pp. 763-766.	
LC	C 16	WALTER, C.D., "Montgomery's Multiplication Technique: How to Make it Smaller and Faster" in Cryptographic Hardware and Embedded Systems - CHAS 1999, C. Paar (Eds.), K. Ko, Ed. 1999, Springer, Berlin Germany, pp.61-72.	
LC	C 17	OH, H. and MOON, J., "Modular Multiplication Method" IEE Proc.-Comput. Digit.Tech., Vol. 145, No. 4, (July 1998), pp. 317-318.	
LC	C 18	BLUM, T., "Modular Exponentiation on Reconfigurable Hardware" Master's thesis, ECE Department, Worcester Polytechnic Institute, Submitted to Faculty 1999-04-08, Published May 1999. Retrieved from the Internet <URL: http://www.wpi.edu/pubs/ETD/Available/etd-090399-090413/unrestricted/blum.pdf>.	
LC	C 19	MARWEDEL, P., et al. "Built in Chaining: Introducing Complex Components into Architectural Synthesis." April 1996. Proceedings of the ASP-DAC, 1997. [online]. Retrieved from the Internet <URL: http://eldorado.uni-dortmund.de:8080/FB4/Is12/forshung/1997/aspdac/aspacPDF>.	
LC	C 20	TIOUNTCHIK, A., and TRICHINA, E., "RSA Acceleration with Field Programmable Gate Arrays" Lecture Notes in Computer Science, Vol. 1587, pp.164-176. Retrieved from the Internet: <URL:http://citeseer.nj.nec.com/274658.html>.	

Examiner Signature		Date Considered	12/16/04
--------------------	--	-----------------	----------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.